TO: The FPKI Policy Authority (FPKIPA)

FROM: The FPKI Management Authority (FPKIMA)
               On behalf of the FPKI Technical Working Group (TWG)

DATE: April 26, 2013

RE: **FPKI PD-VAL Validation Report**
               Ascertia ADSS SCVP Server 4.5.1.4

The FPKIMA completed Path Discovery and Validation (PD-VAL) testing of *Ascertia's Advanced Digital Signature Services (ADSS) Server-based Certificate Validation Protocol (SCVP) Server* in accordance with the FPKI PD-VAL Product Conformance Testing Process.

The FPKI TWG has evaluated the test results detailed in the *FPKI PD-VAL Product Conformance Technical Test Report [Ascertia ADSS SCVP Server]; Version 1.1.0; June 14, 2012* and recommends that the FPKIPA approve this product for the FPKI PD-VAL Product List (PPL) with the following specifications:

- Product Vendor/Organization Name: *Ascertia*
- Product Identification: *ADSS SCVP Server, Patch Version 4.5.1.4, Build 4514.4510.280312.9150*
- Product Description: *SCVP Server*
- Provides Path Discovery Services (Yes/No): *Yes*
- Provides Path Validation Services (Yes/No): *Yes*
- Testing Process: *FPKI PD-VAL Product Conformance Testing Process; Version 1.0.0; Dated January 7, 2013*
- Associated Test Suites: National Institute of Standards and Technology (NIST) PKI test suites:
    a. Public Key Interoperability Test Suite (PKITS) for Certification Path Validation; Version 1.0.1; April 14, 2011
        i. NIST Recommendation for X.509 Path Validation
    b. Path Discovery Test Suite; Version 0.1.1; June 3, 2005

- The applicable FPKI PD-VAL Conformance Testing Categories and Optional FPKI PD-VAL Services are denoted in the table below with ☑:

FPKI PD-VAL Supported Services	Conformance Testing Category			
	Dynamic Path Validation	Static Path Validation	Path Discovery	Path Discovery and Validation
Baseline FPKI PD-VAL Service	☑	☑	☑	☑
Optional FPKI PD-VAL Services				
Products that support delta-CRLs	☑	☑	N/A	N/A
Products that can process a nameRelativeToCRLIssuer in the cRLDistributionPoint and issuingDistributionPoint	☑	☑	N/A	N/A
Products that process indirect CRLs	☑	☑	N/A	N/A
Products that process the onlySomeReasons field of the issuingDistributionPoint extension	☑	☑	N/A	N/A
Products that can set initial-policy-set to "any-policy" when initial-explicit-policy is set	☑	☑	N/A	N/A
Products that support DSA signatures	☑	☑	N/A	N/A
Products that support DSA signatures and parameter inheritance	☑	☐	N/A	N/A
Products that support the mixed use of UTF8String encoding & PrintableString encoding in the certificates	☑	☑	N/A	N/A
Products that support case insensitive matching between the issuer field of an end entity certificate and the corresponding subject field of the CA certificate, using UTF8String encoding	☑	☑	N/A	N/A
Products that support: dnQualifier, serialNumber, & ST in the certificate Subject Name	☑	☑	N/A	N/A
Products that support: T (Title), generationQualifier, pseudonym, SN, initials, givenName, and L (Locality) in the certificate Subject Name	☐	☑	N/A	N/A
Products that gracefully handle User Notice Qualifier text with more than 200 characters	☑	☑	N/A	N/A
Products that support mesh environments with a mix of URI types in the certificates, including no AIA or SIA in the certificates and CRLs issued by the CAs closest to the trust anchor	N/A	N/A	☑	☐

FPKIPA Chair Approval

By digitally signing this memo, the FPKIPA Chair approves the FPKI TWG recommendation to include ***Ascertia's Advanced Digital Signature Services (ADSS) Server-based Certificate Validation Protocol (SCVP) Server*** on the FPKI PPL with the specifications listed above.

This approval does not apply to subsequent product versions, testing process versions, or test suite versions. This approval applies only to the FPKI PD-VAL Conformance Testing Categories and Optional FPKI PD-VAL Services check marked above.

_____ _____
Deb Gallagher, FPKIPA Chair   Date